DATA PROTECTION ANNEX

CITY OF HELSINKI

Version update 14 February 2019

1. Definitions

(1) **Subcontractor** means subcontractors of the Supplier, as defined in the Main Agreement.

(2) **Personal Data** means, in accordance with Article 4, paragraph 1 of the General Data Protection Regulation, personal data that the Customer has disclosed to the Supplier, or which the Customer has saved in the Service, or which have been created in the production of the Service, or which the Supplier has in some other way gained access to while producing the Service, and which the Supplier processes on the part of the Customer and on behalf of it.

(3) **Processing of personal data** means, in accordance with Article 4, paragraph 2 of the Data Protection Regulation, any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(4) **Service** means the service, project, collaboration, system or supply procurement or other operations, which the Customer and the Supplier have agreed upon in the Main Agreement.

(5) **Main Agreement** means the agreement between the Customer and the Supplier as defined in paragraph 2 (1), and its annexes.

(6) **Contracting Parties** means the **Customer** and the **Supplier** as defined in the Main Contract.

(7) **Data Protection Regulation** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

(8) **Data Protection Annex** means this document, which is enclosed to the Main Agreement.

2. General obligations of the Contracting Parties

(1) The Contracting Parties have signed the Main Agreement [add the subject of the agreement, agreement number, date of signature], through which the Contracting Parties have agreed upon the production of the Service. In the production of

the Service, the Supplier and its Subcontractors shall comply with this Data Protection Annex and the Customer's data security directives.

(2) The Supplier shall be responsible for ensuring that the confidentiality, availability or integrity of the Personal Data is not compromised due to negligence, incorrect methods or other activities undertaken by the personnel of the Supplier at variance with this Data Protection Annex or the Main Agreement.

(3) The Customer shall be responsible for ensuring that its operations are carried out in accordance with this Data Protection Annex and the data protection legislation, and strive in all reasonable manners to contribute to the Supplier's possibilities to act in accordance with this annex.

(4) In spite of what may have been agreed upon in the Main Agreement or in other contract documents between the Contracting parties concerning the matters covered in this Data Protection Annex or the responsibilities connected to them or the relative order of validity between the contract documents, this Data Protection Annex is always the primary source applied to the matters covered in this Data Protection.

3. Subcontracting

(1) Without written consent from the Customer, the Supplier may not use subcontractors other than the Subcontractors defined in the Main Agreement for the processing of Personal Data. The Supplier shall, without undue delay, inform the Customer in writing about all planned changes, which concern the adding or changing of Subcontractors that process Personal Data.

(2) The Supplier shall make sure that it can adhere to the conditions of this Data Protection Annex, also when using Subcontractors.

(3) The Supplier shall be responsible for ensuring that its Subcontractors act in accordance with this Data Protection Annex. The Supplier shall be responsible for its Subcontractors in the same way it is responsible for its own operations. The Supplier shall be responsible for ensuring that the Customer’s right of inspection is also extended to the Supplier’s Subcontractors.

(4) The obligations set in this Data Protection Annex for the personnel of the Supplier shall also be applied to the Subcontractor's personnel that participate in the production of the Service.

4. Processing of Personal Data

(1) The Customer is the controller of Personal Data in accordance with the Data Protection Regulation and responsible for the processing of this data. The Supplier and its Subcontractors are processors of Personal Data as referred to in the Data Protection Regulation. The Supplier shall be obliged to adhere to all the obligations imposed on processors of Personal Data in the Data Protection Regulation, and in other existing legislation at a given time, and ensure in the agreements concerning subcontracting that its Subcontractors adhere to them.

(2) The Contracting Parties shall agree separately upon the following matters:

a. The subject of the processing (which data the agreement applies to) and the duration (the term of the agreement)
b. The nature of the processing (what kind of processing is agreed upon, e.g. collection/saving of data) and purpose (why Personal Data is processed, what the purpose of the processing of Personal Data is according to the agreement)
c. Type of Personal Data (which Personal Data is processed, e.g. name, address information) and groups of the data subjects (who are in the register, e.g. clients / special categories of personal data in accordance with article 9, whose processing shall be based on special grounds)

(3) The Supplier shall process Personal Data on behalf of the Customer only to the extent it is necessary for the production of the Service and only until the period of validity of the Main Agreement has expired or the Suppliers duty to help and assist has expired in accordance with the directions of the Customer. The Supplier shall not be entitled to use the Personal Data in its own operations, process them in contravention of this Data Protection Annex, combine Personal Data with other material in its possession or disclose them.

(4) When the Main Agreement expires, the Supplier and its Subcontractors shall return the Customer's material that includes Personal Data and other material that has been allocated by and belongs to the Customer, and erase the data and copies stored in their deposit copies. The Supplier shall be responsible that the Customer’s material is separate or separable from the Supplier’s other material. The material shall not be erased, if the Customer, the law or authority regulations require that it is stored. In that case, the Customer shall provide further directives to the Supplier on how it should act.

(5) The Supplier shall not process, transfer or disclose the Customer's Personal Data outside the EU or EEA area. The servers shall also be located in the EU area or the EEA area, and the Supplier shall inform the Customer of their locations. The Supplier shall inform the Customer in advance, if the location of the

servers changes. If the Main Agreement includes stricter rules concerning the processing or the location of the servers, for example that the servers shall be located in Finland, then the Main Agreement is applied.

(6) If the Supplier processes Personal Data in its own system or in its Subcontractor's system, then the Supplier shall be obliged to save the log data from all processing tasks involving Personal Data, including the viewing of Personal Data. The Supplier shall provide, on request of the Customer, the log data in question to the Customer. More precise terms for the obligations concerning log data are agreed upon in the Main Agreement or its appendices.

(7) The Supplier shall, if needed, assist the Customer in carrying out an assessment of the impact in accordance with Article 35 of the Data Protection Regulation and a prior consultation in accordance with Article 36.

(8) The Supplier shall commit to informing the Customer without undue delay about all requests of the data subjects, which concern the exercise of rights of the data subject according to the Data Protection Regulation and other existing legislation.

(9) The Supplier shall commit to assisting the Customer by means of appropriate technical and organisational measures so that the Customer can fulfil its obligation to answer requests which concern the exercise of rights of the data subject. As a processor of Personal Data, the Supplier understands that requests to exercise these rights may require that it assists the data subject with reporting and communications, exercising the access right of the data subject, correction or erasure of personal data, carrying out a restriction of the processing and/or transferring personal data from a system to another.

(10) In the case of a data security breach, the Supplier shall assist the Customer in preparing an announcement to the supervisory authority and the data subject in accordance with Articles 33 and 34 of the Data Protection Regulation.

5. The Supplier's data security

(1) In order to ensure that the security level corresponds with the risk, the Supplier shall be committed to implement the appropriate technical and organisational measures to ensure that the processing of Personal Data is secure considering new technology and implementation costs, the nature, extent, context and purposes of the processing, as well as the risks of various probability and gravity to the rights and freedoms of natural persons, and to comply with the Customer's directives and possible updates to the Customer's directives.

(2) The Supplier shall be responsible for ensuring that the Service it produces is fault tolerant and that the Personal Data can be restored quickly in case of a physical or technical fault.

(3) In its operations, the Supplier shall regularly and systematically monitor the realisation of the security level required in this Data Protection Annex, register possible deviations and report them to the Customer without delay and start the corrective measures as soon as possible.

(4) Such premises of the Supplier and its Subcontractor, where Personal Data is stored, used or otherwise processed, must be appropriately secured to prevent unauthorised access to the Personal Data.

(5) The Supplier shall be responsible for ensuring that Personal Data is disclosed to, Personal Data can be processed by or access to systems containing Personal Data is given only to designated persons belonging to the personnel of the Supplier and its Subcontractor, who need Personal Data in their work connected to the production of the Service. The Supplier shall be responsible for ensuring that the persons in question adhere to this Data Protection Annex and that the persons in question have signed a written secrecy obligation before they start processing Personal Data or gain access to the aforementioned systems.

6. Processing of data security breaches

(1) The Supplier notifies the Customer of data security breaches relating to the Service immediately when it has learned about them.

(2) The Supplier shall provide the Customer with at least the following information about a data security breach:

- describe the data security breach; if the breach concerns Personal Data, describe, as far as possible, the groups and number of the data subjects concerned as well as the groups and approximated number of types of personal data;

- inform the data protection officer or another person in charge, from whom it is possible to obtain further information;

- describe the probable consequences of the data security breach; and

- describe the measures that the Supplier would suggest or which it has carried out due to the data security breach and, if needed, also the measures to alleviate the potential harmful effects.

If all the above-mentioned data cannot be provided simultaneously, the data can be provided gradually without undue delay.

(3) The Supplier shall be obliged to support the Customer with the minimisation of damages connected to data security breaches.

7. Audit

(1) The Supplier shall be entitled to audit the Service and its delivery and the Supplier's systems in connection to it.

(2) The audit shall be carried out in a way which does not compromise the data security of the Supplier's other customers or the confidentiality of their data.

(3) The Customer shall be responsible for the costs associated with the organisation of the audit.

(4) The Supplier shall rectify the defects discovered in the audit without undue delay. Substantial defects, which pose an obvious threat to the data security, must be rectified immediately.

(5) Defects and errors discovered in the audit that stem from the Supplier's derelictions or errors at variance with the Main Agreement or this Data Protection Annex shall be rectified without charge by the Supplier.